PATCH MANAGEMENT

WHY PATCH MANAGEMENT IS ESSENTIAL?

- **Enhanced Security:** Patch management plays a crucial role in fortifying the security of your organisation by addressing vulnerabilities in your software and applications. This proactive approach helps minimise the risk of cyber-attacks.

- **Optimised System Uptime:** By consistently updating and maintaining software and applications, patch management contributes to seamless operations, minimising disruptions, and supporting overall system uptime.

- **Compliance Assurance:** In the face of escalating cyber threats, regulatory bodies often mandate organisations to uphold specific compliance standards. Patch management is an integral part of meeting these requirements and ensuring adherence to regulatory guidelines.

- **Feature Enhancements:** Beyond addressing bugs, patch management extends to incorporating updates that enhance the features and functionality of your software. Staying on top of patches ensures that your organisation benefits from the latest advancements offered by the products you use.

The NST Solution:

Implementing patch management requires a meticulous organisational process that balances cost-effectiveness and a strong focus on security. At NST, we have dedicated teams committed to executing efficient patch management.

Operating beyond your business hours, our teams rigorously test and apply Microsoft and agreed third-party patches to your fleet, ensuring minimal disruption to your business operations.

sales@nst.com.au | www.nst.com.au

OUR BUSINESS PROCESS

Chances are that your company already employs certain tools and processes. Our team collaborates closely with you to comprehensively grasp your existing tools and processes, aligning them with mutually agreed-upon enhancements. Whether utilising your existing patching tools or integrating ours, we ensure a seamless alignment with your established frameworks.

Introducing Pre-Patch Routine Tasks:

- Thorough review of Microsoft and 3rd Party patch releases
- Monthly generation of a comprehensive patch plan report for stakeholders
- Notification to IT Staff and affected users about planned patch windows and potential impact
- Compilation of an overall patch schedule calendar for the Service Desk to communicate with users
- Comprehensive check of the overall patching system health, including space, schedule, automatic deployment rules, performance, and synchronisation of MS and 3rd Party patches
- Documentation of necessary changes for vulnerability remediation, subject to CAB approval

Enhanced Patch Management Reporting:

- Generate a comprehensive report on the deployment and compliance of Microsoft and 3rd Party patches
- Compile a summary of patch deployment status, outlining successes and any potential issues

Optimising Platform Performance:

- Streamline the WSUS database through optimisation measures
- Purge outdated, superseded, declined, and unused patches to declutter the system
- Remove superseded and unused patches from SCCM software update groups to maintain efficiency
- Conduct a thorough health check for patch distribution points, addressing space issues, faulty packages, and reviewing distribution point logs
- Regularly assess and update patch distribution configurations to align with evolving organisational needs and system demands

Patch Scheduling, Deployment and Testing:

- Verify schedules are correct
- Verify backup health prior to pilot patch deployment and monitor deployment of patches to the pilot workstations group Identify and resolve issues
- Monitor deployment of patches to the production workstation groups
- Post deployment verification tasks
- Assist owners of “critical systems” with application testing after patch deployment and rollback if necessary
- Implement approved changes for vulnerability remediation

Revitalised Patch Scheduling, Deployment, and Testing:

- Validate the accuracy of schedules to ensure precision in the patching process
- Prior to the pilot patch deployment, assess the health of backups and monitor the deployment on the pilot workstations group
- Swiftly identify and address any issues that may arise during the deployment
- Monitor the seamless deployment of patches to the production workstation groups
- Post-deployment verification tasks to ensure the effectiveness of the applied patches
- Collaborate with owners of “critical systems” for thorough application testing post-patch deployment, with a provision for rollback if necessary
- Execute approved changes essential for vulnerability remediation in a timely manner

sales@nst.com.au | www.nst.com.au